AD-A043 731 CLEMSON UNIV S C DEPT OF MATHEMATICAL SCIENCES F/G 12/1

A NOTE ON POLYNOMIAL MATRIX FUNCTIONS OVER A FINITE FIELD.(U)

AUG 77 J V BRAWLEY N00014-76-C-0130

UNCLASSIFIED TR-256 NL

| OF |

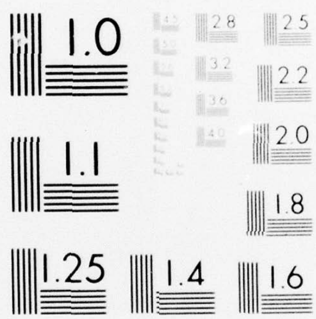
AD A043731

END

DATE FILMED

9-77

DDC


1.0
2.8
2.5
3.2
2.2
3.6
4.0
2.0
1.1
1.8
1.25
1.4
1.6

DEPARTMENT
OF
MATHEMATICAL
SCIENCES

CLEMSON UNIVERSITY
Clemson, South Carolina

A NOTE ON POLYNOMIAL MATRIX FUNCTIONS OVER A FINITE FIELD

BY

J. V. BRAWLEY*

DEPARTMENT OF MATHEMATICAL SCIENCES
CLEMSON UNIVERSITY

TECHNICAL REPORT #256
CONTRACT REPORT N8

*RESEARCH SUPPORTED BY
THE OFFICES OF NAVAL RESEARCH
CONTRACT N00014-76-C-0130

A Note on Polynomial Matrix Functions

over a Finite Field

by J.V. Brawley*

1. Let $F = GF(q)$ denote the finite field of order q, and let F_n denote the ring of nxn matrices over F. Consider an element $A(x) \varepsilon F_n[x]$; i.e.,

$$A(x) = A_N x^N + A_{N-1} x^{N-1} + \ldots A_1 x + A_0 \tag{1}$$

where $A_i \varepsilon F_n$. This polynomial defines via substitution several functions from F_n to F_n. Two such functions are

$$B \rightarrow A_r(B) = A_N B^N + A_{N-1} B^{N-1} + \ldots + A_1 B + A_0 \tag{2}$$

and

$$B \rightarrow A_L(B) = B^N A_N + B^{N-1} A_{N-1} + \ldots + BA_1 + A_0 \text{ .} \tag{3}$$

We call (2) and (3), respectively, the right and left polynomial functions determined by $A(x)$ with the terms right and left indicating the side on which the substituting variable is placed.

---

*Supported in part by ONR contract N00014-76-C-0130.

Definition. A function $A: F_n \to F_n$ is called a right respectively left) polynomial function if there exists a polynomial $A(x) \in F_n[x]$ which represents A via the right subsitution (2) (respectively(3)).

In this note we obtain unique representations for and determine the number of right (left) polynomial functions $A: F_n \to F_n$. Proofs will be given for the right functions which can be obviously modified for the left polynomial functions.

2. Recall that

$$L_n(x) = \prod_{i=1}^{n} (x^{q^i} - x) \tag{4}$$

is the monic polynomial of least degree in F[x] satisfied by every $B \in F_n$; indeed, $L_n(x)$ is the least common multiple of all degree n polynomials in F[x] [See, 2]. We define δ by

$$\delta = \deg L_n(x) = q^n + q^{n-1} + \ldots + q. \tag{5}$$

THEOREM 1. Let $Z(x) = \sum_{i=0}^{N} Z_i x^i$ be a polynomial in $F_n[x]$ with $\deg Z(x) = N < \delta$. If $Z_r(B) = Z_N B^N + \ldots + Z_1 B + Z_0 = 0$ for every $B \in F_n$, then $Z_i = 0$, $i = 0, 1, 2, \ldots, N$.

Proof. Let $f(x) = x^n - a_{n-1}x^{n-1} - \ldots - a_1 x - a_0$ be an arbitrary polynomial of degree n in F[x], and let $C \in F_n$ denote the companion matrix of f(x). Dividing Z(x) by f(x) we obtain

$$Z(x) = Q(x)\, f(x) + R(x) \tag{6}$$

where $Q(x)$ and $R(x)$ are in $F_n[x]$ with

$$R(x) = R_{n-1}x^{n-1} + \ldots + R_1x + R_0 \ . \tag{7}$$

Since $f(x)$ is a scalar polynomial we may substitute an arbitrary matrix B into (6) to get $Z_r(B) = Q_r(B)f(B) + R_r(B)$. In particular, for every nonsingular $P \in GL(n,q)$ it follows from the Hamilton-Cayley theorem that

$$0 = Z_r(PCP^{-1}) = R_r(PCP^{-1}) \ .$$

Thus $(R_r(PCP^{-1}))P = 0$ or

$$R_{n-1}PC^{n-1} + R_{n-2}PC^{n-1} + \ldots + R_1PC + R_0P = 0 \tag{8}$$

for every $P \in GL(n,q)$.

Now it is known [1] that each matrix $X \in F_n$ can be written as a linear combination of nonsingular matrices P_i; i.e.,

$$X = c_1P_1 + c_2P_2 + \ldots + c_tP_t \ , \ c_i \in F.$$

If follows from (8) that

$$R_{n-1}XC^{n-1} + R_{n-2}XC^{n-1} + \ldots + R_1XC + R_0X = 0 \tag{9}$$

for every $X \in F_n$. In particular, if we take $X = E_m$ where E_m has a 1 in position $(m,1)$ and zeros elsewhere we find through actual computation that equation (9) reduces to

$$\begin{pmatrix} r_{1m}^{(0)} & r_{1m}^{(1)} & \cdots & r_{1m}^{(n-1)} \\ r_{2m}^{(0)} & r_{2m}^{(1)} & \cdots & r_{2m}^{(n-1)} \\ \vdots & \vdots & & \vdots \\ r_{nm}^{(0)} & r_{nm}^{(1)} & & r_{nm}^{(n-1)} \end{pmatrix} = 0$$

where $R_k = (r_{ij}^{(k)})$. Thus column m of R_k is zero for $k = 0, 1, \ldots, n-1$ and $m = 1, 2, \ldots, n$; i.e., $R_k = 0$ for $k = 0, 1, \ldots, n-1$. It follows from (6) that $f(x)$ divides $Z(x)$ for every monic of degree n; hence $L_n(x)$ divides $Z(x)$. But $\deg Z(x) < \deg L_n(x)$ so $Z(x)$ must be the zero polynomial; i.e., every $Z_i = 0$ and the proof is complete.

As a corollary to Theo[illegible] we have the following:

THEOREM 2. <u>Each right polynomial function</u> $A:F_n \to F_n$ <u>can be represented uniquely by a polynomial</u> $A(x) \in F_n[x]$ <u>of degree</u> $< \delta$ <u>and each such polynomial represents a right polynomial function. The number of right polynomial functions is therefore</u> $q^{n^2\delta}$.

Proof. If $A_1(x)$ and $A_2(x)$ have degree $< \delta$ and each represent the right polynomial function A then $A_1(x) - A_2(x)$ represents the zero function; hence by Theorem 1, $A_1(x) = A_2(x)$.

Finally let A be a right polynomial function and let $A(x)$

represent A. By division

$$A(x) = Q(x)L_n(x) + R(x)$$

where $R(x)$ has degree $< \delta$. Clearly, $R(x)$ represents A.

References

1. J. V. Brawley. On the ranks of basis of vector spaces of matrices. Linear Algebra and Its Applications. 3(1970), 51-55.

2. J. V. Brawley, L. Carlitz, and Jack Levine. Scalar polynomial functions on the $n \times n$ matrices over a finite field. Linear Algebra and Its Applications. 10(1975), 199-217.

Unlimited

Security Classification

DOCUMENT CONTROL DATA - R & D

(Security classification of title, body of abstract and indexing annotation must be entered when the overall report is classified)

1. ORIGINATING ACTIVITY (Corporate author)
Department of Mathematical Sciences
Clemson University
Clemson, South Carolina

2a. REPORT SECURITY CLASSIFICATION
Unclassified

2b. GROUP

3. REPORT TITLE
(6) A NØte on Polynomial Matrix Functions Over a Finite Field

4. DESCRIPTIVE NOTES (Type of report and inclusive dates)
(9) Technical rept.

5. AUTHOR(S) (First name, middle initial, last name)
(10) J. V. Brawley

(14) TR-256, CR-N8

6. REPORT DATE
8/1/77 (11) 1 Aug 77

7a. TOTAL NO. OF PAGES
5

7b. NO. OF REFS
2

8a. CONTRACT OR GRANT NO.
(15) N00014-76-C-0130

b. PROJECT NO.

c.

d.

9a. ORIGINATOR'S REPORT NUMBER(S)
N8

9b. OTHER REPORT NO(S) (Any other numbers that may be assigned this report)
(12) 8p.

10. DISTRIBUTION STATEMENT
Unlimited

11. SUPPLEMENTARY NOTES

12. SPONSORING MILITARY ACTIVITY

407 183

13. ABSTRACT

Let $F = GF(q)$ denote the finite field of order q, and let F_n denote the ring of $n \times n$ matrices over F. Each matrix polynomial $A(x) = A_N x^N + \ldots + A_1 x + A_0$ in $F_n[x]$ defines via substitution several functions from F_n to F_n. Two such functions, called respectively, the right and left polynomial functions determined by A(x) are

$$B \to A_r(B) = A_N B^n + \ldots + A_1 B + A_0$$

$$B \to A_L(B) = B^n A_N + \ldots + BA_1 + A_0$$

A function $A: F_n \to F_n$ is called a right (left) polynomial function if there exists $A(x) \in F_n[x]$ which represents A via the right (left) substitution $B \to A_r(B)$ $(B \to A_L(B))$. This paper obtains a unique representation for and determines the number of right (left) polynomial functions $A: F_n \to F_n$.

DD FORM 1473 1 NOV 65 (PAGE 1) PLATE NO. 21856

S/N 0102-014-6600

Unclassified

Security Classification